Substitution table L

	1	2	3	4	5	6	7
1	2	7	5	1	3	6	4
2	4	1	2	5	7	3	6
3	7	5	1	2	6	4	3
4	1	6	3	7	4	5	2
5	3	2	6	4	1	7	5
6	6	4	7	3	5	2	1
7	5	3	4	6	2	1	7

Encrypt

PT : 34

key 71

CT ??

$3 \oplus 7 = ?$

$4 \oplus 1 = ?$

Recall

$p \oplus k = z$

Decrypt

PT ???

key 315

CT 315

$? \oplus 3 = 3$

$? \oplus 1 = 1$

$? \oplus 5 = 5$

Find key

PT	73
key	??
CT	65

$7 \oplus ? = 6$

$3 \oplus ? = 5$

Sub Table NL

	a	b	c	d	e
a	e	b	b	d	c
b	b	d	a	a	e
c	c	e	d	c	a
d	a	c	e	b	d
e	d	a	c	e	b

Decrypt:

	? ?
key	b e
	a a

Find key:

PT	b e
key	? ?
CT	a a

Find key: PT: b a

key: ? ?

---

c d

Encrypt using NS_1

	0	1	2	3	4
0	4	1	0	3	2
1	2	3	0	1	4
2	1	4	3	2	0
3	0	2	4	1	3
4	3	0	2	4	1

PT 1 4

key 2 3

CT ? ?

$1 \oplus 2 = ?$

$4 \oplus 3 = ?$

Find another PT s.t

PT ? ?

key 2 3

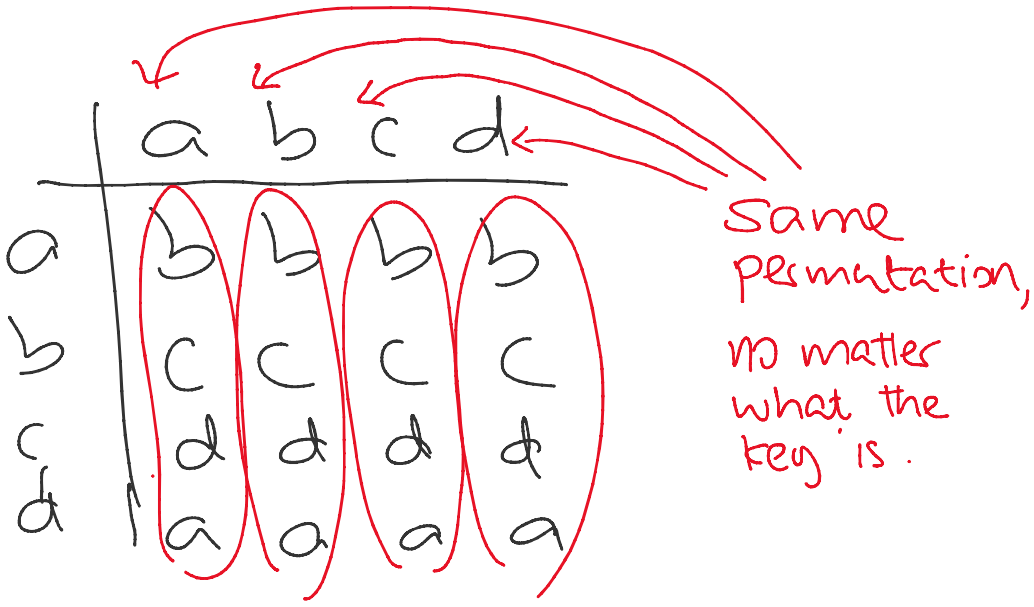
CT 0 4

Conclusion For the table

NS1 decryption is not unique. So it is not suitable for encryption purposes.

The reason is that some of the columns contain repetitions.

Another non-Latin Sub table



⇝ This stream cipher is "key independent".

This is indeed a substitution cipher on the alphabet

$$\{a, b, c, d\}$$

with permutation $(bcda)$

Exercise Show that any substitution cipher on any alphabet can be described as a stream cipher.